Subject: - **Cyber Security Advisory – Apple iPhones Targeted with Blast Pass Exploit to Deploy Pegasus Spyware (Advisory No. 56)**

05 OCT 2023

Context. Reportedly, Apple iPhone users are being targeted by NSO Group's nefarious Spyware i.e. Pegasus. The exploitation process is instigated through iMessage feature (CVE-2023-41061 and CVE-2023-41064) for deployment of Blast Pass (zero day and zero click malware).

2. **Blast Pass Exploit**. Blast Pass is capable of infecting OS latest versions (16.6) without user interaction. In this regard, Apple has issued remedial advisory for iPhone users. Apple has also generated alerts to inform its users for being targeted by NSO Pegasus spyware or likely targeted by state-sponsored attackers. Apple users are urged to follow safety steps mentioned at para-3 to prevent against Blast Pass Pegasus exploit and other prevalent cyber-attacks.

3. **Specific Safety Steps to Blast Pass Exploit**

a. Immediately upgrade to iOS latest version (16.6.1 or above) which covers majority of security updates related to ongoing attacks.

b. Enable lockdown mode (optional; extreme protection mode) to block Blast Pass attack.

c. Disable iMessage feature available in iPhones.

4. **Generic Security Steps for Apple Users**

a. Protect devices with strong passcodes and use two factor authentications on Apple ID.

b. Install apps from official Apple Store only to avoid malware/infection.

c. Use anonymity-based solutions (over internet while surfing) and mask identity of key appointment holders/individuals.

d. Always disable location from Apple devices.

e. Subscribe to Apple's security bulletins, threat notifications and auto OS update features.

f. Strictly avoid using phones at sensitive locations/meetings.

3. Kindly disseminate the above information to all concerned in your organizations, all attached/affiliated departments and ensure necessary protective measures.